CLAIMS

1. A method of universal calculation on points on an elliptic curve, characterised in that the elliptic curve is defined by a quartic equation and in that identical programmed calculation means are used to carry out an operation of addition of points, an operation of doubling of points, and an operation of addition of a neutral point, the calculation means comprising in particular a central processing unit (2) associated with a memory (4, 6, 8).

2. A method according to Claim 1, characterised in that the elliptic curve is defined by a quartic equation of the type:

$$V^2 = b.U^4 + a.U^3W + UW^3,$$

(U : V : W) being Jacobi projective coordinates of a point P on the elliptic curve, and a, b being parameters of the elliptic curve, a point with coordinates (0 : 0 : 1) being a neutral point O of the elliptic curve, a point with coordinates (U : -V : W) being an inverse point (-P) of the point P with coordinates (U : V : W).

3. A method according to Claim 2, in which the point P is also defined in affine coordinates (X, Y), the affine coordinates (X, Y) and the Jacobi projective

coordinates (U : V : W) of the point P being linked by the relationships:

$$(X, Y) = (U/W, V/W^2).$$

4. A method according to Claim 2 or 3, in which, in order to carry out the addition of a first point P1 defined by first Jacobi projective coordinates (U1 : V1 : W1) and a second point P2 defined by second Jacobi projective coordinates (U2 : V2 : W2), the coordinates of the first point P1 and those of the second point P2 being stored in first and second registers in the memory (4, 6, 8), the first point and the second point belonging to the elliptic curve,

the programmed calculation means calculate third Jacobi projective coordinates (U3 : V3 : W3) defining a third point P3, the result of the addition, by the following equations:

$$U3 = 2.b.U1^2.U2^2 + (aU1.U2 + W1.W2).(U1.W2+W1.U2) + 2V1.V2$$

$$\begin{aligned} V3 = {} & (U1^2.V2+U2^2.V1)* \\ & (4b.(U1.W2+U2.W1).W1.W2 \\ & - 8b^2.(U1.U2)^2 \\ & + a.[(2W1.W2)^2 - (aU1.U2+W1.W2)^2] \\ & + (W1^2.V2+W2^2.V1)* \end{aligned}$$

$$[(aU1.U2+W1.W2)^2-(2aU1.U2)^2 + 4bU1.U2.(W1.U2+U1.W2)] - 4bU1.U2.(U1.W1.V2+U2.W2.V1)(aU1.U2-W1.W2)$$

$$W3 = (aU1.U2-W1.W2)^2 - 4bU1.U2(U1.W2+U2.W1)$$

and then store the third projective coordinates (U3 : V3 : W3) in third registers in the memory (6, 8).

5. A method according to Claim 1, in which the elliptic curve is a curve comprising a single point of order two and is defined by a quartic equation of the type:

$$V^2 = \varepsilon.U^4 - 2\delta.U^2.W^2 + W^4,$$

(U : V : W) being Jacobi projective coordinates of a point P on the elliptic curve, and ε, δ being parameters of the elliptic curve, the point with coordinates (0 : 1 : 1) being the neutral point O of the elliptic curve, the point with coordinates (-U : +V : W) being the inverse point (-P) of the point P (U : V : W).

6. A method according to Claim 5, in which, in order to carry out the addition of the first point P1 defined by first Jacobi projective coordinates (U1 : V1 : W1) and the second point P2 defined by second Jacobi projective coordinates (U2 : V2 : W2), the coordinates of the first point P1 and those of the second point P2

being stored in first and second registers in the memory (4, 6, 8), the first point and the second point belonging to the elliptic curve,

the programmed calculation means calculate third Jacobi projective coordinates (U3 : V3 : W3) defining a third point P3, the result of the addition, by the following equations:

$$U3 = U1.W1.V2 + V1.U2.W2$$

$$V3 = [(W1.W2)^2 + \varepsilon(U1.U2)^2] * [V1.V2 - 2\delta U1.U2.W1.W2] + 2\varepsilon.U1.U2.W1.W2(U1^2W2^2 + W1^2U2^2)$$

$$W3 = (W1.W2)^2 - \varepsilon(U1.U2)^2$$

and then store the third projective coordinates (U3 : V3 : W3) in the third registers in the memory (6, 8).

7. A method according to one of Claims 5 to 6, in which the elliptic curve is defined in affine coordinates by an equation of the type:

$$Y^2 = \varepsilon.X^4 - 2\delta.X^2 + 1$$

(X, Y) being affine coordinates of a point P on the elliptic curve.

8. A method according to Claim 7, in which, in order to carry out the addition of the first point P1 defined by first affine coordinates (X1, Y1) and the second point P2 defined by second affine coordinates (X2, Y2), the coordinates of the first point P1 and those of the second point P2 being stored in first and second registers in the memory (4, 6, 8), the first point P1 and the second point P2 belonging to the elliptic curve,

the programmed calculation means calculate third affine coordinates (X3, Y3) defining a third point P3, the result of the addition, by the following equations:

$$X3 = (X1.Y2 + Y1.X2)/[1 - \varepsilon(X1.X2)^2]$$

$$Y3 = \{[1+\varepsilon(X1.X2)^2].[Y1.Y2 - 2\delta.X1.X2]+2\varepsilon.X1.X2.(X1^2+X2^2)\} / [1 - \varepsilon(X1.X2)^2]$$

and then store the third affine coordinates (X3, Y3) in the third registers in the memory (6, 8).

9. A method according to one of Claims 5 to 8, in which the elliptic curve is a curve comprising three points of order two and has $\varepsilon = 1$ as a parameter.

10. Use of a calculation method according to one of Claims 1 to 9 in a scalar multiplication calculation method applied to points on an elliptic curve.

11. Use of a calculation method according to one of Claims 1 to 9 in a cryptographic method.

12. An electronic component comprising programmed calculation means for implementing a method according to one of Claims 1 to 9, the calculation means comprising in particular a central processing unit (2) associated with a memory (4, 6, 8).

13. An electronic component comprising means for implementing a cryptographic algorithm using a method according to one of Claims 1 to 9.

14. A smart card comprising an electronic component according to Claim 12 or 13.